MINUTES
Strategic Planning Committee

DATE	June 19, 2002
TIME	10:00 AM
LOCATION	Kinkead Building, 6th Floor Conference Room Carson City
RECORDER	Alisanne Maffei, Strategic Planner

ATTENDEES

Name	Attend ✓	Name	Attend ✓
Chair – Mike Hillerby, Governor's Office	✓	Co-Chair – Mark Blomstrom, DoIT	✓
Chuck Chinnock, Taxation	✓	Terry Savage, DoIT	✓
Jim Demme, NDOT		Scott Sisco, Cultural Affairs	✓
Myla Florence, DETR	✓	Tom Stephens, NDOT	
Sara Jones, Cultural Affairs	✓	P. Forrest Thorne, PEBS	✓
Alisanne Maffei, DoIT	✓	Doug Walther, B&I	
John E. Neill, NDOT	✓	Ginny Lewis, DMV	
Pam V. Sutton, DoIT	✓	Dana Mathiesen, DMV	
Kathy Ryan, DoIT	✓	Freeman Johnson, CNR	

CALL TO ORDER

I Introduction

- Mike Hillerby opened the meeting stating he would need to leave to attend a previously scheduled Board of Education meeting before the Committee's Gartner Presentation on Security.

II Review and Approval of the Minutes.

- After review of the March meeting minutes, it was motioned by Scott Sisco to accept the minutes and seconded by Terry Savage. There were no other comments. The minutes from March 20, 2002, were accepted as presented.

III DISCUSSION

NITOC Top-10 IT Issues comparison

Alisanne Maffei walked through the comparison of the NITOC and Strategic Planning Committee Top-10 IT Issues. The Top Ten Issues were very similar between the two groups. Some Issues as in IT Salary and Training were not ranked high by the Strategic Planning Committee because they view the IT Workforce Committee to be addressing those issues.

Mike Hillerby made the comment that NITOC represents specific committees and so they would have more specific concerns such as Architecture, whereas the Strategic Planning Committee is comprised of major departments, not based on issues. There was a consensus that the two committees were not far off from each other.

- Gartner Research Group Presentation on Information Security Management

  In preparation for the Gartner Research Group Presentation to be made to the Committee, three slides were distributed: The Information Security Validation Steps (Steps 1 – 6: Information Security Policy and Standards, Information Security Architecture and Processes, Information Security Awareness and Training, Auditing Monitoring and Investigating, Validation);Business Continuity Components (Disaster Recovery, Business Recovery, Business Resumption, and Contingency Planning) and Overall Recommendations.

  Myla Florence inquired if the Security Committee was developing a model for agencies to use. Terry Savage responded yes, the Security has worked on the basic PSP's (Policy, Standards and Procedures) as in Step1 and will now move to Step 2 (Security Architecture).

  The Committee requested that Donna Crutcher, Chair of the IT Security Committee, attend the next Strategic Planning Committee Meeting to discuss what the Security Committee is doing. Mike Hillerby stated he would be interested in how we'll be able to implement the security PSP's with in budget impacts. Terry Savage stated that they are coming up with a clear set of bullet points of the top security issues agencies need to be aware of and would be able to present these issues to non-IT individuals.

  An overview from Gartner Research Group on Information Security Management commenced with the Gartner Analyst, Matt Easley presenting the topic.

  Terry Savage asked "how do you sell the need for IT Security to non-IT people or the Legislature? Are there any success stories in Government?"

  The Gartner Analyst responded "get the money amounts on where we have had incidents and the impact, and define some scenarios with possible costs. Look at exposure that recently occurred. Estimate if half the cost is up front, it is twice that amount spent to fix the problem.

Gartner is seeing across the board, including government, the use of outsourcing the monitoring of security systems with security providers. The ROI to keeping the bad guys out is there.

Additional areas were discussed

Host Intrusion Protection – to protect against internal malicious acts, using new technologies.

Monitoring external and internal security

Intrusion Detection Systems –changing to be able to halt a detected intrusion, not just send an alert.

Firewall Technology – firewalls act as security guards, blocking or granting network access to users based on security policies, they restrict network access by screening traffic passing between insecure networks and secure networks

Applications and Interface weaknesses

External Attack forces open ports - Should a hacker breach the firewall, the hacker takes all—the networks to which it connects will be open to various malicious hacking activities

Terry Savage asked what trends and growth rates are seen in actual attacks?

The analyst responded that the growth on internet attacks has slowed in the past year. The reporting is getting better, improving the statistics.

Percentage 100%	Types of Attacks
53%	Internal Authorized Employees
20%	Unauthorized Employees
12%	Former Employees
15%	Hackers/Competitors

John Neil asked what types of employee attacks are occurring. The analyst replied that access to resources not related to their business functions is a large component. John asked if there any statistics on what types of data they are after, such as HR material. Perhaps this is a focus of more service areas? The analyst states "identify which resources are most important; Layer resources to these resources and use an Intrusion Detection System (IDS).

Specific examples of Employee Breeches will be disclosed at the next meeting (i.e.: installation/use of unauthorized software, use of computing resources for illegal activities, and use of computing resources for personal profit.)

· E-gov Strategic Plan Presentation

Pam Sutton presented the e-gov Strategic Plan to the Committee and requested further input. Pam reviewed the e-gov strategic plan objectives, pertinent definitions and composition of the constituents. She outlined the guiding principles and areas addressed in the plan. The eight major areas addressed are: Enterprise Approach, Policy, Planning, Legislation, Funding, Privacy/Security/Accessibility, Architecture/Infrastructure, and Streamlined Business Processes.

Pam reviewed the Enterprise Approach as a fundamental area the other areas hinge upon.

It was noted that both the Top-10 IT Issues listings identify e-gov as one of the areas of high priority.

IV WRAP UP

The next meeting of the IT Strategic Planning Committee will be August 7, 2002 in the 6th floor HR Conference Room.

. .

ACTION ITEMS

Item No.	Description	Assigned To
1.	Create a proposal to draft a pilot program and research into lease agreement providing IT hardware, software, and periodic replacement on a statewide basis for submittal to the Legislature.	Mark Blomstrom, Alisanne Maffei
2.	Report on examples of Employee Breeches	Alisanne Maffei
3.	Invite Donna Crutcher, IT Security Committee Chair, to present an update and discuss what the Security Committee is doing.	Mark Blomstrom, Alisanne Maffei
4.	Provide input on e-gov Strategic Plan at next meeting.	All